

AMENDMENTS TO THE DRAWINGS

The attached sheets of drawings correct reference characters and typographical errors in FIGs. 1, 2, 4, 5, and 8, and to add the legend “Related Art” to FIG. 1.

Attachments: Five (5) Replacement Sheets (FIGs. 1, 2, 4, 5, and 8)
Five (5) Annotated Sheets (FIGs. 1, 2, 4, 5, and 8)

REMARKS/ARGUMENTS

In this Amendment Under 37 C.F.R. § 1.111 (“Amendment”), Applicant amends the specification in order to improve clarity. Applicant also amends the drawings to correct reference characters and typographical errors in FIGs. 1, 2, 4, 5, and 8, and to add the legend “Related Art” to FIG. 1. Additionally, Applicant amends claims 8 and 51 to recite, inter alia, “for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier” in order to better define the claimed invention. Further, Applicant amends claims 25 and 29 to change dependency. Moreover, Applicant makes other amendments to claims 1, 5-9, 11, 16, 17, 19, 23-27, 29, 30, and 36-61 in order to improve clarity. No new matter is introduced.

Applicant makes no amendments in response to the Examiner’s rejections under 35 U.S.C. § 103(a).

Prior to entry of the Amendment, claims 1-61 were pending in the application. After entry of the Amendment, claims 1-61 remain pending in the application.

In the Office Action, the Examiner rejected claims 20, 22, 25, 26, and 29 under 35 U.S.C. § 112, ¶ 2; rejected claims 8-41 and 51-55 under 35 U.S.C. § 101; rejected claims 8-17, 23, 27, and 51-54 under 35 U.S.C. § 103(a) as being unpatentable over “New VLSI Architecture of RSA Public-Key Cryptosystem” by Wang et al. (“Wang”); and rejected claims 19-22, 25, and 26 under 35 U.S.C. § 103(a) as being unpatentable over Wang in view of U.S. Patent No. 5,796,645 to Peh et al. (“Peh”).

Applicant respectfully traverses the Examiner’s rejections under 35 U.S.C. § 103(a).

Drawings

The attached sheets of drawings correct reference characters and typographical errors in FIGs. 1, 2, 4, 5, and 8, and to add the legend “Related Art” to FIG. 1.

Applicant requests that the Examiner indicate the updated status of the drawings in the next paper mailed by the U.S. Patent and Trademark Office.

Claim Rejection Under 35 U.S.C. § 112, ¶ 2

Applicant submits that one of ordinary skill in the art would understand the term “full compressor”, as used in the present application, to mean a device that inputs a first number of values and outputs a second number of values, where the first number is larger than the second number. Similarly, Applicant submits that one of ordinary skill in the art would understand the term “reduced compressor”, as used in the present application, to mean a device that inputs a third number of values and outputs the second number of values, where the first number is larger than the third number, and where the third number is larger than the second number.

Applicant amends claim 25 to depend from claim 20, and amends claim 29 to depend from claim 28.

Applicant submits that this discussion and these amendments obviate the Examiner’s rejection under 35 U.S.C. § 112, ¶ 2.

Claim Rejection Under 35 U.S.C. § 101

Applicant amends independent claims 8 and 51 to recite, inter alia, “for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier”.

Applicant submits that claims 8 and 51, at least as amended, accomplish a practical application; that the practical application yields a real-world result that is useful, tangible, and concrete; and that claims 8 and 51 do not cover every substantial practical application. As a result, Applicant submits that these amendments obviate the Examiner's rejection under 35 U.S.C. § 101.

Claim Rejections Under 35 U.S.C. § 103(a)

Applicant submits that the Examiner has failed to establish a proper prima facie case of obviousness for at least the following reason.

Applicant submits that FIG. 5 of Wang discloses two carry save adders, the first one higher and to the left, the second one lower and to the right. Wang, FIG. 5. The first carry save adder appears to receive a value $(-B, 0, B, 2B)$ from the left MUXs, while the second carry save adder appears to receive a value $(-N, 0, N, 2N)$ from the right MUXs. Id. The first carry save adder also appears to receive output from the second carry save adder, while the second carry save adder also appears to receive output from the first carry save adder. Id.

Thus, contrary to the allegations of the Office Action (p. 4, ¶ 6), Wang does not disclose “an accumulator including a carry save adder inherently having a plurality of compressors . . . each of the plurality of compressors receiving a multiple modulus (a multiple of N from MUXs), a partial product (a multiple of B from MUXs), a corresponding current sum and a corresponding current carry (the feedback from the carry save adder), and producing a corresponding next sum and a corresponding next carry (the output from the carry save adder)” (emphases added).

Applicant notes that the Examiner does not argue that Peh overcomes this deficiency of Wang.

As a result, Applicant submits that independent claims 8 and 51 are patentable under 35 U.S.C. § 103(a) over Wang or any proper combination of Wang, Peh, and the other art of record. Applicant further submits that dependent claims 9-41 and 52-55 are patentable under 35 U.S.C. § 103(a) over Wang or any proper combination of Wang, Peh, and the other art of record, at least for the same reason that claims 8 and 51 are patentable, from which claims 9-41 and 52-55 directly or indirectly depend.

Request for Reconsideration and Allowance

Accordingly, in view of the above amendments and remarks, reconsideration of the rejections and allowance of each of claims 1-61 in connection with the present application is earnestly solicited.

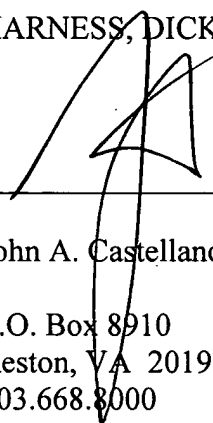
Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

If necessary, the Director of the USPTO is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; in particular, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By


John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, VA 20195
703.668.8000

JAC/LFG/cm